Infraestrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 2 – Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Leitoras de Cartões Inteligentes no Âmbito da ICP-Brasil

Versão 3.1

Brasília, 26 de setembro de 2017

SUMÁRIO

Controle de Versão

Versão atual	Data de emissão	Alterações realizadas
2.0.r.6	07/06/06	Revisões de ambiente operacional (seção 2.1.6) Revisões de classe de operação para cartão e leitora (seção 3.5 REQUISITO III.20). Revisão das funcionalidades do papel de acesso "usuário" (seção 2.2.12 REQUISITO II.21). Inclusão do termo "Módulo criptográfico multiaplicação" no glossário.
3.0.r.09	22/11/07	Revisão geral para os requisitos de cartões criptográficos ICP e leitoras de cartões inteligentes. Exclusão dos requisitos de *tokens* criptográficos. Revisão estrutural do Manual de Condutas Técnicas incluindo no desenvolvimento do mesmo documento os requisitos técnicos para cartões criptográficos ICP, leitoras de cartões inteligentes e materiais a serem depositados para a execução do processo de homologação.
3.1 IN 08/2017	26/09/2017	Previsão de autonomia para o OCP definir os ensaios nas Avaliações de Manutenção de Credenciamento.

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

1 Introdução

Este documento descreve os procedimentos de ensaio a serem aplicados no processo de homologação de leitoras de cartões inteligentes no âmbito da Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de ensaio referem-se ao conjunto de métodos que serão usados para avaliar se leitoras de cartões inteligentes estão ou não em conformidade com os requisitos técnicos definidos pelo Manual de Condutas Técnicas 2 - Volume I.

Em um Credenciamento Inicial e na Avaliação de Recertificação devem ser aplicados todos os ensaios definidos neste MCT. Em cada Avaliação de Manutenção, cabe ao OCP definir quais requisitos devem ser ensaiados. Uma Avaliação de Manutenção deve observar a proporção mínima de 20% (vinte por cento) do total dos requisitos previstos neste MCT para cada avaliação de manutenção no modelo 4 e de 33% (trinta e três por cento) do total dos requisitos previstos neste MCT para cada avaliação de manutenção no modelo 5. A avaliação de um requisito em uma Avaliação de Manutenção não impede sua reavaliação em Avaliações de Manutenção seguintes, mas ao longo das Avaliações da Manutenção o OCP deve garantir que todos os requisitos deste MCT sejam avaliados.

Para uma melhor compreensão do disposto neste documento, entenda-se por leitora de cartão inteligente um hardware instalado no computador que utiliza uma conexão física do tipo Serial (RS232) ou USB, que serve de interface de interação entre o cartão inteligente e uma aplicação.

1.1 Organização deste Documento

Cada seção deste documento contém um conjunto de requisitos que representam citações diretas do próprio texto do Manual de Condutas Técnicas 2 – Volume I. Os requisitos estão organizados da seguinte forma:

- *REQUISITO <número_do_requisito>.<número_de_seqüência_do_requisito>*
  - "número_do_requisito": corresponde ao número de área definido no Manual de Condutas Técnicas 2 – Volume I;
  - "número_de_seqüência_do_requisito": corresponde a um identificador seqüencial dos requisitos.

Os procedimentos de ensaio visam orientar sobre como proceder nos testes elaborados sobre dispositivos. Os procedimentos de ensaio estão classificados e agrupados por Níveis de Segurança de Homologação da seguinte forma:

- NSH 1: Este nível não requer depósito e análise de código fonte associado ao dispositivo em homologação;
- NSH 2: Este nível requer depósito e análise de apenas código fonte de componentes específicos associados ao dispositivo em homologação. Por exemplo, código fonte do algoritmo gerador de números pseudo-aleatórios;
- NSH 3: Este nível requer depósito e análise de código fonte completo associado ao dispositivo em homologação. Por exemplo, código fonte de todo software e/ou firmware do módulo criptográfico.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista LEA estão organizados da seguinte forma:

- *EN.<número_do_requisito>.<número_de_seqüência_do_requisito>.<número_de_seqüência_do_ensaio>*
  - "número_do_requisito";
  - "número_de_seqüência_do_requisito";
  - "número_de_seqüência_do_ensaio": corresponde a um identificador seqüencial dos procedimentos que devem ser desempenhados.

Este documento (MCT 2 – Volume II) está estruturado da seguinte forma:

- Parte 1: Descreve os procedimentos de ensaio que devem ser verificados no processo de homologação de leitoras de cartões inteligentes.

2 Parte 1

Procedimentos de ensaios a serem observados no processo de homologação de leitoras de cartões inteligentes no âmbito da ICP-Brasil

2.1 Introdução

Esta parte apresenta os procedimentos de ensaios que devem ser verificados no processo de homologação de leitoras de cartões inteligentes.

Os procedimentos de ensaios descritos nesta parte englobam:

- Recomendações de segurança;
- requisitos de interoperabilidade;
- requisitos de documentação.

2.2 Recomendações de segurança

As recomendações de segurança descrevem mecanismos de segurança adicionais que podem estar implementados em leitoras de cartões inteligentes com a finalidade de proteger dados críticos de identificação e autenticação da entidade usuária externa pela leitora, como por exemplo, o PIN. Mecanismos de segurança adicionais implementados em leitoras de cartões inteligentes podem ser:

- Teclado numérico isolado (PIN *pad*) para a entrada de dados numéricos que serão enviados ao cartão inteligente para fins de identificação e autenticação da entidade usuária externa;
- teclado alfanumérico isolado para a entrada de dados alfanuméricos que serão enviados ao cartão inteligente para fins de identificação e autenticação da entidade usuária externa;
- dispositivo biométrico isolado para fins de identificação e autenticação da entidade usuária externa no cartão inteligente;
- tela (*display*) isolada para a apresentação de dados críticos de segurança que são gerados pelo cartão inteligente.

REQUISITO I.1: Caso a leitora de cartões inteligentes suporte mecanismos de segurança adicionais, então o envio de dados críticos de segurança ao cartão inteligente para fins de identificação e autenticação da entidade usuária externa deve estar sob controle exclusivo da leitora.

Procedimentos de Ensaio para NSH 1:

EN.I.01.01: Verificar se a documentação técnica descreve os mecanismos de segurança adicionais da leitora e os métodos de manipulação dos dados críticos.

EN.I.01.02: Por análise direta da leitora e de seu projeto de hardware, verificar as funcionalidades dos mecanismos de segurança adicionais.

EN.I.01.03: Realizar operações que envolvem o uso dos mecanismos de segurança adicionais, e por meio de aplicação específica, analisar o tráfego de dados na interface de comunicação entre a leitora e o PC, verificando se há o envio de dados críticos pela leitora ao PC.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.01.04: Por análise direta do código-fonte do firmware e driver da leitora, verificar se os métodos de manipulação de dados críticos são controlados exclusivamente pela leitora.

REQUISITO I.2: A documentação técnica deve descrever os mecanismos de segurança que estejam implementados na leitora, incluindo:

- Algoritmos criptográficos e protocolos utilizados para troca segura de informações entre o dispositivo de entrada (PIN pad, teclado alfanumérico ou dispositivo biométrico) e o cartão inteligente;
- mecanismos de cachê de dados de autenticação;
- realimentação de dados de autenticação (*echo*) para uma entidade usuária externa de forma obscura durante a autenticação (por exemplo, nenhuma exibição legível de caracteres no momento da inserção de um PIN);
- mecanismos utilizados para que dados de autenticação manipulados pela leitora estejam protegidos contra leitura não autorizada;
- mecanismos de segurança física utilizados para prevenir acesso físico não autorizado aos componentes da leitora;
- mecanismos que mitigam ataques, como por exemplo, proteção contra vazamento de informações por emanações eletromagnéticas (*Electromagnetics Attacks – EMA*) ou por consumo de corrente (*Differential Power Analysis – DPA*).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.02.01: Verificar se a documentação técnica atende ao **REQUISITO I.2**.

2.3 Requisitos de Interoperabilidade

REQUISITO II.1: Leitoras de cartões inteligentes, sempre que aplicável a cada caso, devem atender aos requisitos de interoperabilidade ora estabelecidos, derivados e complementares aos padrões ISO/IEC 7816 e PS/SC versão 1.0, conforme descrito nos itens a seguir.

Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.3.**

2.3.1 Interface física entre leitoras e cartões inteligentes

Esta seção determina os requisitos de interoperabilidade e compatibilidade que devem ser atendidos por leitoras e cartões inteligentes no que diz respeito a interface física entre eles. Tais requisitos foram derivados dos padrões ISO/IEC 7816-2 e PC/SC versão 1.0, a saber:

- *Interoperability Specification for ICCs and Personal Computer Systems - Part 2*. "*Interface Requirements for Compatible IC Cards and Readers*";
- ISO/IEC 7816-2 *Identification cards – Integrated circuit(s) cards with contacts – Part 2*: *Dimensions and location of the contacts* – ISO/IEC 7816-2.

2.3.1.1 Requisitos de interface física

2.3.1.1.1 Atribuição de contatos elétricos

REQUISITO II.2: Os contatos elétricos localizados em uma leitora de cartões inteligentes devem ser compatíveis com os requisitos definidos na seção 5 do padrão ISO/IEC 7816-2 e identificados conforme mostra a Tabela 1.

Tabela 1. Identificação dos contatos para leitoras de cartões inteligentes

Identificação do contato	Descrição
C1	Voltagem de alimentação (*supply voltage* – Vcc)
C2	Sinal "reset" (RST)
C3	Sinal "clock" (CLK)
C4	Reservado para uso futuro em outras partes do ISO/IEC 7816 (não usado atualmente) - RFU (*reserved for future use*)
C5	terra – "ground" (GND)
C6	Identificado pelo padrão ISO/IEC 7816-2 como "voltagem de programação" (*variable supply voltage* - VPP) – geralmente não mais usado
C7	entrada/saída de dados (d*ata input*/o*utput* – I/O)
C8	reservado para uso futuro em outras partes do ISO/IEC 7816 (não usado atualmente) - RFU (*reserved for future use*)

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.02.01: Verificar se a documentação técnica descreve a atribuição de contatos elétricos da leitora de cartões inteligentes. Este requisito não é testado separadamente e faz parte da **Seção 2.3**.

OBSERVAÇÃO: Para leitoras de cartões inteligentes, os contatos elétricos C4, C6 e C8 podem ser considerados opcionais. Entretanto, para fins de compatibilidade com alguns tipos de cartões inteligentes, alguns destes contatos podem ser utilizados possuindo, como por exemplo, a finalidade de fornecer uma alimentação auxiliar para cartões de memória.

REQUISITO II.3: Caso os contatos C4, C6 e C8 não sejam necessários, então devem estar isolados, do ponto de vista elétrico (não condutíveis), dos circuitos integrados e de quaisquer outros contatos inseridos na leitora. Caso os contatos C4, C6 ou C8 sejam utilizados para uma finalidade específica, a documentação técnica deve descrever a finalidade de uso e características dos respectivos contatos.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.03.01: Verificar se a documentação técnica descreve como os contatos elétricos não usados são eletricamente isolados em leitoras de cartões inteligentes.

EN.II.03.02: Analisar se os contatos elétricos não usados estão eletricamente isolados entre si e com relação aos demais, medindo tal isolamento por meio de experimentação na leitora de cartões inteligentes, e verificar a ausência de ligação elétrica dos contatos não usados.

EN.II.03.03: Ativar a leitora de cartões inteligentes, colocando em modo de operação, e verificar por meio de medida experimental a ausência de ligação elétrica com os contatos não usados.

REQUISITO II.4: Os contatos elétricos da leitora de cartões inteligentes devem seguir as disposições definidas na seção 4 da ISO/IEC 7816-2, conforme apresentado na Figura 1.

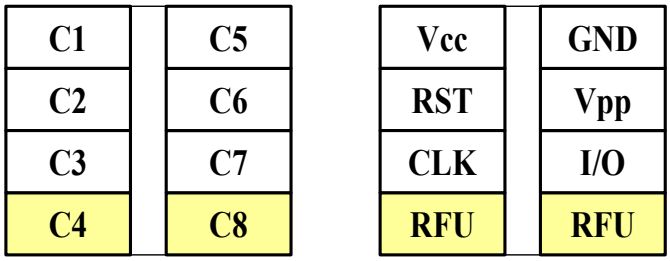

Figura 1. Numeração dos contatos elétricos para leitoras de cartões inteligentes segundo padrão ISO/IEC 7816-2

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.04.01: Verificar se a documentação técnica descreve a disposição dos contatos elétricos na leitora de cartões inteligentes. Este requisito não é testado separadamente e faz parte da **Seção 2.3.**

REQUISITO II.5: A documentação técnica deve descrever a identificação dos contatos elétricos presentes na leitora de cartões inteligentes.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.05.01: Verificar se a documentação técnica descreve a identificação dos contatos elétricos na leitora de cartões inteligentes. Este requisito não é testado separadamente e faz parte da **Seção 2.3.**

2.3.1.1.2 Inserção e remoção de cartões inteligentes

As recomendações e requisitos descritos a seguir devem ser atendidos por leitoras que usam mecanismos de inserção e remoção manuais.

RECOMENDAÇÃO II.1: É recomendado que leitoras sejam projetadas para posicionar cartões inteligentes de tal forma que sempre estejam acessíveis por seus respectivos proprietários.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.REC.II.01.01: Verificar se a documentação técnica descreve se as leitoras foram projetadas para posicionar cartões inteligentes de tal forma que sempre estejam acessíveis por seus respectivos proprietários.

EN.REC.II.01.02: Verificar, por inspeção, se o cartão inteligente encontra-se sempre acessível ao seu respectivo proprietário quando conectado à leitora.

RECOMENDAÇÃO II.2: Para facilitar a popularização deste tipo de dispositivo, é recomendado que leitoras tenham mecanismos manuais simples de inserção e remoção de cartões inteligentes.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.REC.II.02.01: Verificar se a documentação técnica descreve se as leitoras possuem mecanismos manuais simples de inserção e remoção de cartões inteligentes.

EN.REC.II.02.02: Verificar, por inspeção, se a leitora possui mecanismos manuais simples de inserção e remoção de cartões inteligentes.

REQUISITO II.6: Leitoras devem assegurar que quaisquer objetos ou materiais físicos, tais como, mas não limitados a sinais indicativos, grampos, parafusos, braçadeiras, pinças, rolos e cilindros, não danifiquem um cartão inteligente, particularmente nas áreas reservadas para tarjas magnéticas e saliências de identificação do proprietário.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.16.01: Verificar se a documentação técnica descreve se as leitoras foram projetadas para assegurar que quaisquer objetos ou materiais físicos não danifiquem um cartão inteligente, particularmente nas áreas reservadas para tarjas magnéticas, saliências de identificação do proprietário e contatos.

EN.II.16.02: Verificar, por inspeção, se um cartão inteligente de teste é danificado, por qualquer objeto ou material físico, ao ser inserido e/ou removido da leitora.

EN.II.16.03: Verificar, por inspeção direta no interior da leitora, se há algum objeto que possa oferecer riscos de danos físicos ao cartão inteligente quando inserido e/ou removido da leitora.

REQUISITO II.7: A documentação técnica deve descrever quais mecanismos de inserção e remoção de cartões inteligentes são suportados pela leitora.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.17.01: Verificar se a documentação técnica atende ao **REQUISITO II.17**.

REQUISITO II.8: Quando aplicável, a documentação técnica deve especificar quais mecanismos de inserção e remoção de cartões inteligentes são suportados pela leitora.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.18.01: Verificar se a documentação técnica atende ao **REQUISITO II.18**.

2.3.2 Propriedades elétricas

Em conformidade com o padrão ISO/IEC 7816-3, duas classes de operação são definidas para representar a voltagem de alimentação (Vcc) aplicada por leitoras em cartões inteligentes:

- Classe A: 5V;
- classe B: 3V.

Além disso, existem outros requisitos técnicos relacionados às propriedades elétricas entre leitoras e cartões inteligentes:

- Método de seleção da classe de operação executado pela leitora;
- valores definidos com relação à voltagem e corrente elétrica.
- freqüência de operação;

REQUISITO II.9: Uma leitora de cartões inteligentes deve atender aos requisitos de propriedades elétricas definidos na seção 4 do padrão ISO/IEC 7816-3. Para leitora de cartões inteligentes, no mínimo, a classe de operação A deve ser suportada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.09.01: Verificar se a documentação técnica descreve as propriedades elétricas da leitora de cartões inteligentes.

EN.II.09.02: Fazer medições elétricas usando equipamentos específicos de bancada de testes (por exemplo, fontes de alimentação, geradores de função e multímetro), visando obter valores de tensão, corrente e frequência. Uma vez que as medições elétricas foram realizadas, verificar se há conformidade com os valores referenciados na seção 4 do padrão ISO/IEC 7816-3.

REQUISITO II.10: A documentação técnica da leitora deve descrever qualquer propriedade elétrica suportada que seja adicional ou não compatível aos requisitos definidos na seção 4 do padrão ISO/IEC 7816-3.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.10.01: Verificar se a documentação técnica atende ao **REQUISITO II.10**.

2.3.3 Transferência de dados em cartões inteligentes

A comunicação com um cartão inteligente é sempre iniciada pela leitora. Desta forma, um cartão inteligente sempre responde a comandos da leitora, nunca enviando dados sem qualquer requisição. Este tipo de relação é denominada de "mestre e escravo", sendo que a leitora desempenha o papel de mestre e o cartão inteligente desempenha o papel de escravo.

Depois que um cartão inteligente for inserido em uma leitora, seus contatos elétricos são mecanicamente conectados aos da leitora. Portanto, os circuitos elétricos da leitora não devem ser ativados até que os contatos do cartão inteligente estejam mecanicamente conectados aos contatos da leitora.

A interação entre a leitora e o cartão inteligente deve ser conduzida por meio das seguintes operações consecutivas:

- Ativação: corresponde à ativação dos circuitos elétricos por parte da leitora;
- troca de informações: corresponde à troca de informações entre cartão inteligente e leitora, sendo que o cartão sempre responde ao estímulo de reinício (*reset*) feito previamente pela leitora;
- desativação: corresponde à desativação dos circuitos elétricos por parte da leitora, devido, por exemplo, à retirada do cartão inteligente.

REQUISITO II.11: A leitora deve atender aos requisitos de ativação dos circuitos elétricos (*cold reset*) definidos na seção 5.3.2 do padrão ISO/IEC 7816-3.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.11.01: Analisar se a documentação técnica descreve os requisitos de ativação dos circuitos elétricos (*cold reset*) conforme a seção 5.3.2 do padrão ISO/IEC 7816-3.

EN.II.11.02: Registrar os sinais elétricos resultantes da ativação dos circuitos elétricos da leitora, por meio de um equipamento específico (por exemplo, um osciloscópio). Uma vez que os sinais elétricos de ativação foram registrados, verificar se há conformidade com a sequência referenciada pela seção 5.3.2 do padrão ISO/IEC 7816-3.

REQUISITO II.12: A leitora deve atender aos requisitos de ativação a quente dos circuitos elétricos (*warm reset*) definidos na seção 5.3.3 do padrão ISO/IEC 7816-3 .

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.12.01: Analisar se a documentação técnica descreve os requisitos de ativação a quente dos circuitos elétricos (*warm reset*) conforme a seção 5.3.3 do padrão ISO/IEC 7816-3.

EN.II.12.02: Registrar os sinais elétricos resultantes da ativação a quente dos circuitos elétricos da leitora, por meio de um equipamento específico (por exemplo, um osciloscópio). Uma vez que os sinais elétricos de ativação foram registrados, verificar se há conformidade com a sequência referenciada pela seção 5.3.3 do padrão ISO/IEC 7816-3.

REQUISITO II.13: A leitora deve atender aos requisitos de desativação dos circuitos elétricos (*deactivation*) definidos na seção 5.4 do padrão ISO/IEC 7816-3 .

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.13.01: Analisar se a documentação técnica descreve os requisitos de desativação dos circuitos elétricos (*deactivation*) conforme a seção 5.4 do padrão ISO/IEC 7816-3.

EN.II.13.02: Registrar os sinais elétricos resultantes da desativação dos circuitos elétricos da leitora, por meio de um equipamento específico (por exemplo, um osciloscópio). Uma vez que os sinais elétricos de ativação foram registrados, verificar se há conformidade com a sequência referenciada pela seção 5.4 do padrão ISO/IEC 7816-3.

2.3.3.1 ATR

DEFINIÇÃO: Com base no padrão ISO/IEC 7816-3, seção 6, subseção 6.1, o ATR (*Answer To Reset*) é o valor da seqüência de bytes enviado pelo cartão inteligente à leitora como resposta ao estímulo de reinício (*reset*) . Neste caso, cada byte é transportado em um caractere assíncrono.

Portanto, conforme mostra a Figura 2, cada estímulo de reinício (*reset*) bem sucedido deve resultar em uma resposta ATR por parte do cartão inteligente. Caso seja necessário fixar alguns parâmetros de transferência de dados que dizem respeito ao protocolo do cartão, uma requisição PPS (*Protocol and Parameters Selection*) pode ser utilizada. Caso contrário, a

leitora analisa o ATR contendo vários parâmetros relacionados ao cartão e à transferência dos dados, e depois envia o primeiro comando a ser processado.

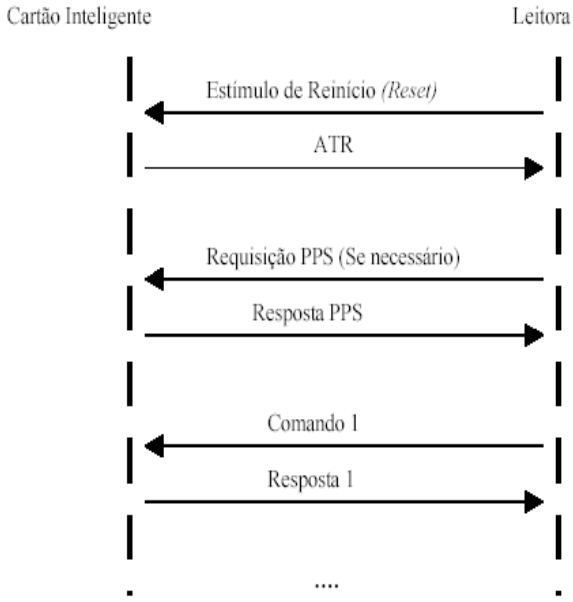

Figura 2. Transferência de dados entre leitora e cartão inteligente

Segundo o padrão ISO/IEC 7816-3, a configuração de um ATR é formada pelos seguintes elementos:

- TS: Caractere inicial;
- T0: Caractere de formato;
- TA(i), TB(i), TC(i) e TD(i): Caracteres de interface;
- T1, T2, ..., TK: Caracteres históricos;
- TCK: Caractere de verificação.

Segundo o padrão ISO/IEC 7816-3, a configuração de uma sequência PPS é formada pelos seguintes elementos:

- PPSS: Caractere inicial;
- PPS0: Caractere de formato
- PPS1, PPS2, PPS3: Caracteres de parâmetro
- PCK: Caractere de verificação

REQUISITO II.14: Leitora de cartões criptográficos ICP devem atender aos requisitos de ATR e PPS de acordo com o padrão ISO/IEC 7816-3 (seções 6 e 7).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.14.01: Analisar se a documentação técnica descreve os requisitos de ATR e PPS da leitora de cartões inteligentes.

EN.II.14.02: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com a leitora de cartões inteligentes, e realizar a ativação e coleta dos dados correspondentes à seqüência ATR enviada por um cartão inteligente de teste. Uma vez que os dados da sequência ATR foram coletados e apresentados pela leitora, verificar se há conformidade com a sequência referenciada pelo padrão ISO/IEC 7816-3 (Seção 6).

EN.II.14.03: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com a leitora de cartões inteligentes, e realizar a ativação de um cartão inteligente de teste que suporte ambos os protocolos T=0 e T=1. Após a ativação do cartão, enviar instruções de baixo nível a leitora para realização de troca de protocolo de comunicação por meio da seqüência PPS entre cartão inteligente e leitora. Verificar se a mudança de protocolo foi processada corretamente por meio do recebimento de uma sequência PPS idêntica como resposta. Uma vez que os dados da sequência PPS foram obtidos indicando o sucesso da operação, verificar se há conformidade com a sequência PPS referenciada pelo padrão ISO/IEC 7816-3 (Seção 7).

2.3.3.2 Protocolos de transmissão de dados

A comunicação com um cartão inteligente pode ser implementada de diversas maneiras por meio de protocolos de transmissão de dados envolvendo o envio de comandos, as respectivas respostas e procedimentos usados quando da ocorrência de erros de transferência de dados.
De acordo com o padrão ISO/IEC 7816-3, há um total de 15 protocolos de transmissão definidos para permitir a comunicação com cartões inteligentes, a saber:

- T=0: faz referência à transmissão assíncrona do tipo "*half-duplex*" orientada a caracteres;
- T=1: faz referência à transmissão assíncrona do tipo "*half-duplex*" orientada a blocos;
- T=2 e T=3: reservados para operações futuras do tipo "*full-duplex*";
- T=4: reservado para uma transmissão assíncrona do tipo "*half-duplex*" e também orientada a caracteres, representando uma versão estendida do protocolo T=0;
- T=5 a T=13: reservados para uso futuro;

- T=14: faz referência aos protocolos de transmissão não padronizados pelo ISO/IEC JTC 1 SC 17 (em alguns casos, T=14 é usado para atender funções nacionais);
- T=15: não faz referência a um protocolo de transmissão, mas, de acordo com o padrão ISO/IEC 7816-3 (seção 6), somente qualifica bytes de interface global.

Destes protocolos de transmissão definidos pelo padrão ISO/IEC 7816-3, dois deles são mais usados em âmbito internacional: T=0 e T=1.

REQUISITO II.15: Uma leitora de cartões inteligentes deve atender aos requisitos de protocolo de transmissão T=0 definidos pelo padrão ISO/IEC 7816-3 (seção 8).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.15.01: Analisar se a documentação técnica descreve os requisitos suportados quanto ao protocolo de transmissão T=0.

EN.II.15.02: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com a leitora de cartões inteligentes, e solicitar o envio de instruções PPS pela leitora ao cartão, por meio de ferramenta específica, para definir o protocolo de transmissão T=0 (padrão ISO/IEC 7816-3 - Seção 8). A seguir, enviar comandos APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

EN.II.15.03: Por meio de ferramenta específica, estabelecer comunicação por meio da interface PC/SC e driver da leitora, e estabelecer conexão lógica com a leitora especificando o protocolo de transmissão T=0 (padrão ISO/IEC 7816-3 - Seção 8). A seguir, enviar comandos APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

REQUISITO II.16: Uma leitora de cartões inteligentes deve atender aos requisitos de protocolo de transmissão T=1 definidos pelo padrão ISO/IEC 7816-3 (seção 9).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.16.01: Analisar se a documentação técnica descreve os requisitos suportados quanto ao protocolo de transmissão T=1.

EN.II.16.02: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com a leitora de cartões inteligentes, e solicitar o envio de instruções PPS pela leitora ao cartão, por meio de ferramenta específica, para definir o protocolo de transmissão T=1 (padrão ISO/IEC 7816-3 - Seção 9). A seguir, enviar comandos APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

EN.II.16.03: Por meio de ferramenta específica, estabelecer comunicação por meio da interface PC/SC e driver da leitora, e estabelecer conexão lógica com a leitora especificando o protocolo de transmissão T=1 (padrão ISO/IEC 7816-3 - Seção 9). A seguir, enviar comandos APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

REQUISITO II.17: A documentação técnica da leitora deve descrever os protocolos de transmissão suportados em conformidade com o padrão ISO/IEC 7816-3 seções 8 e 9.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.17.01: Verificar se a documentação técnica atende ao **REQUISITO II.17**.

2.3.4 Conexão de leitoras em computadores pessoais

Esta seção detalha os requisitos de interoperabilidade que devem ser atendidos por leitoras de cartões inteligentes quando conectadas em computadores pessoais (PC – *Personal Computers*). Tais requisitos foram derivados do padrão PC/SC versão 1.0, de dezembro de 1997, a saber:

- *Interoperability Specification for ICCs and Personal Computer Systems - Part 3*. "*Requirements for PC-Connected Interface Devices*";
- *Interoperability Specification for ICCs and Personal Computer Systems - Part 4*. "*IFD Design Considerations and Reference Design Information*".

Os requisitos de interoperabilidade necessários para uma leitora estão concentrados em três componentes (veja Figura 3):

- Leitora: dispositivo físico que provê a interface com um cartão inteligente;
- driver de Leitora: corresponde a um driver instalado no PC que permite ao sistema operacional e outros componentes de software se comunicarem com a leitora (dispositivo de hardware);
- módulo de Interface: corresponde à interface de programação hospedada em um PC que realiza interações entre o componente "Driver de Leitora" e as camadas superiores.

Portanto, conforme ilustrado na Figura 3, esta seção restringe seu escopo em especificar requisitos de interoperabilidade que estão relacionados a:

- Leitora;
- driver de leitora;
- módulo de interface;
- funcionalidades do módulo de interface.

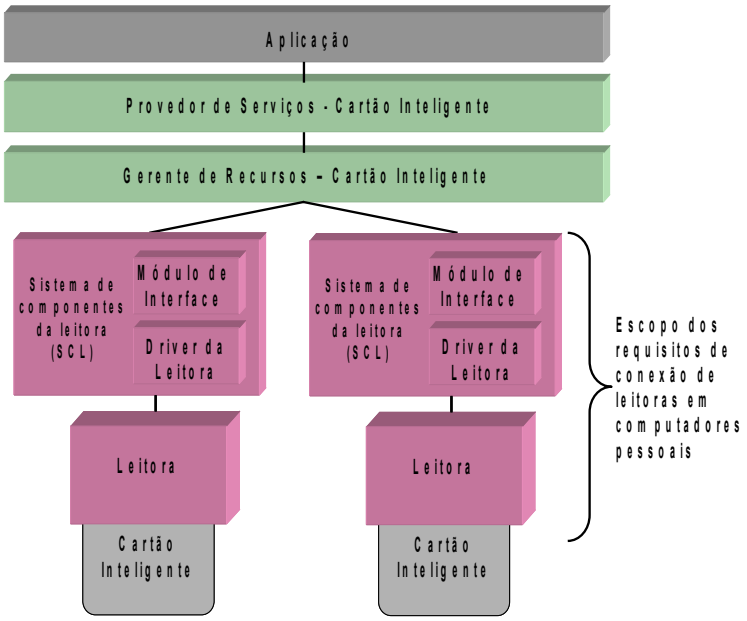

Figura 3. Componentes de leitoras que devem atender aos requisitos de interoperabilidade especificados

2.3.4.1 Leitora

REQUISITO II.18: A leitora se conecta a um PC como um dispositivo periférico devendo atender aos seguinte requisitos:

- Suportar comunicações de dados bidirecionais entre um cartão inteligente e um PC;
- incorporar as funcionalidades necessárias para suportar a interface disponível pelo componente "módulo de interface".

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.18.01: Verificar se a documentação técnica descreve os métodos de conexão entre a leitora e um PC.

EN.II.18.02: Observar, por meio de ferramenta específica, a comunicação entre uma leitora de cartões inteligentes e o PC, enviando comandos a leitora e recebendo as respectivas respostas em baixo nível. Após observar as trocas de informações entre a leitora e o PC, verificar que a comunicação é bidirecional.

EN.II.18.03: Quanto às funcionalidades necessárias para suportar a interface disponível pelo componente "Módulo de Interface", este ensaio é verificado como parte das **Seções 2.3.4.3 e 2.3.4.4** deste documento.

2.3.4.2 Driver Leitora

REQUISITO II.19: Com relação ao canal de entrada e saída de dados (I/O) em um PC, pelo menos, uma das seguintes interfaces deve ser suportada pela leitora e seu respectivo driver:

- PS/2 (interface integrada ao teclado);
- RS-232 (interface do tipo porta serial);
- placa com interface adaptada;
- interface do tipo porta paralela;
- interface de PC baseada em cartão externo (PCMCIA de computadores portáteis (*laptops*), por exemplo);
- interface SCSI;
- interface USB.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.19.01: Verificar se a documentação técnica descreve as interfaces suportadas pela leitora e seu respectivo driver.

EN.II.19.02: Verificar, por meio da observação direta dos conectores e processo de instalação do driver, se a leitora suporta, pelo menos, uma das interfaces mencionadas no **REQUISITO II.19**.

RECOMENDAÇÃO II.3: Considerando leitoras de cartões inteligentes com interface USB, é recomendado, para fins de interoperabilidade, a implementação do padrão USB CCID Revisão 1.1 [CCID 1.1].

Procedimentos de Ensaio para NSH 1:

EN.II.19.01: Verificar se a documentação técnica descreve a compatibilidade da leitora de cartões inteligentes com o padrão USB CCID Revisão 1.1.

EN.II.19.02: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com a leitora de cartões inteligentes, e enviar instruções conforme o padrão USB CCID Revisão 1.1. Uma vez que os dados das respostas a estas instruções foram obtidos, verificar a conformidade com o padrão USB CCID Revisão 1.1.

Procedimentos de Ensaio para NSH 2 e 3:

EN.II.19.03: Verficar, por meio da análise direta do código fonte do driver da leitora a conformidade com o padrão USB CCID Revisão 1.1.

2.3.4.3 Módulo de interface

O módulo de interface corresponde a um software sendo executado em um PC que implementa uma interface padrão e independente tanto do hardware quanto do canal de I/O. Além disso, o módulo de interface também deve mapear as funcionalidades disponíveis pela leitora.

REQUISITO II.20: A parte interessada possui a responsabilidade de criar os componentes "driver de leitora" e "módulo de interface", de tal forma que seja possível aos SPs (*Service Providers*) se comunicarem com um cartão inteligente por meio da leitora.

Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.3.4**.

REQUISITO II.21: Drivers de leitoras de cartões inteligentes devem prover mecanismos de tratamento de erros.

Procedimentos de Ensaio para NSH 1:

EN.II.21.01: Analisar a documentação técnica referente a este requisito, e verificar se consta a descrição dos mecanismos de tratamento de erros relacionados ao driver da leitora.

EN.II.21.02: Provocar erros relacionados ao driver da leitora, e verificar se os mecanismos de tratamento de erros atuaram conforme documentação.

Procedimentos de Ensaio para NSH 2 e 3:

EN.II.21.03: Verficar, por meio da análise direta do código fonte do driver da leitora, se os mecanismos de tratamento de erros estão implementadas conforme documentação.

2.3.4.4 Funcionalidades do módulo de interface

As funcionalidades descritas a seguir estão relacionadas aos requisitos de interoperabilidade, e devem estar visíveis por meio do componente "módulo de interface".

2.3.4.4.1 Funcionalidades obrigatórias

A - Características Operacionais

REQUISITO II.22: Em um dado instante, o módulo de interface deve suportar, no mínimo, uma conexão lógica e ativa entre uma aplicação e a leitora. Em outras palavras, o módulo de interface não necessita suportar múltiplas conexões ativas com uma aplicação. Entretanto, tal funcionalidade não deve impedir o gerenciamento de sessões conforme as características definidas pelo padrão ISO/IEC 7816-4.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.22.01: Verificar se a documentação técnica descreve o gerenciamento de sessões conforme as características definidas pelo padrão ISO/IEC 7816-4.

EN.II.22.02: Via API, estabelecer uma conexão lógica e ativa entre uma aplicação e a leitora, conforme os passos descritos a seguir:

- Obter a lista de todas as leitoras suportadas pelo PC;
- Estabelecer uma conexão com uma leitora escolhida.

EN.II.22.03: Baseando-se no ensaio **EN.II.22.02**, verificar que foi possível estabelecer uma conexão lógica com sucesso.

REQUISITO II.23: Se um módulo de interface suportar múltiplas leitoras, ele deve apresentar uma conexão lógica independente para cada leitora. Além disso, neste caso, o módulo de interface deve também suportar uma funcionalidade que possibilite determinar a associação entre uma dada leitora e sua respectiva conexão lógica.
A implementação de características relacionadas ao gerenciamento de sessões deve estar sob a responsabilidade do cartão inteligente e seu respectivo provedor de serviços (SP – *Service Provider*).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.23.01: Verificar se a documentação técnica descreve o gerenciamento de múltiplas leitoras pelo módulo de interface.

EN.II.23.02: Considerando múltiplas leitoras conectadas num PC, via API, estabelecer uma conexão lógica e ativa entre uma aplicação e cada leitora conectada. Em seguida, para as conexões lógicas estabelecidas com sucesso, verificar que tais conexões são independentes para cada leitora.

EN.II.23.03: Considerando múltiplas leitoras conectadas a um PC, verificar se o módulo de interface permite, por meio de uma funcionalidade específica, associar uma conexão lógica estabelecida com uma dada leitora conectada.

REQUISITO II.24: A documentação técnica da leitora deve descrever as características operacionais que estão implementadas no dispositivo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.24.01: Verificar se a documentação técnica atende ao **REQUISITO II.24.**

B – Enumeração das funcionalidades da leitora

REQUISITO II.25: O componente "Módulo de interface" deve prover uma interface que suporte a enumeração de funcionalidades (obrigatórias e opcionais). Tal interface deve estar disponível para requisição via SP do cartão inteligente.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.25.01: Analisar a documentação técnica referente a este requisito, verificando as funcionalidades que podem ser enumeradas do módulo de interface.

EN.II.25.02: Via ferramenta específica, verificar se o módulo de interface permite, por meio de invocação de função em sua interface, enumerar as funcionalidades suportadas (obrigatórias e opcionais).

REQUISITO II.26: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.2, tabela 3-1, no mínimo, uma invocação via SP deve retornar informações sobre:

- Fornecedor da leitora;
- comunicação;
- protocolos;
- gerenciamento de energia;
- características de garantia de segurança;
- características mecânicas;
- características específicas do fornecedor.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.26.01: Analisar a documentação técnica referente a este requisito, verificando as informações que podem ser retornadas por meio de uma invocação via SP.

EN.II.26.02: Por meio de ferramenta específica, deve verificar se, no mínimo, as informações descritas no **REQUISITO II.26** são retornadas por invocação via Provedor de Serviços.

EN.II.26.03: Baseando-se no ensaio **EN.II.26.02**, verificar se as informações retornadas estão em conformidade com o padrão PC/SC versão 1.0, Parte 3, Seção 3.1.2 e Tabela 3-1.

REQUISITO II.27: A documentação técnica da leitora deve descrever todas as funcionalidades disponíveis no dispositivo, mostrando de forma clara a estrutura de dados utilizada (TLV, por exemplo).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.27.01: Verificar se a documentação técnica atende ao **REQUISITO II.27.**

REQUISITO II.28: A documentação técnica da leitora deve descrever as versões dos seguintes componentes:

- Hardware;
- software;
- firmware.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.28.01: Verificar se a documentação técnica atende ao **REQUISITO II.28.**

REQUISITO II.29: A parte interessada deve prover os meios necessários para identificação pela entidade usuária externa das versões dos seguintes componentes da leitora:

- Hardware;
- software;
- firmware.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.29.01: Verificar se a documentação técnica atende ao **REQUISITO II.29.**

C – Eventos relacionados a um cartão inteligente

REQUISITO II.30: Considerando cartões inteligentes, dois tipos de eventos devem ser detectados pela leitora:

- Notificação de inserção do cartão inteligente;
- notificação de remoção do cartão inteligente.

O componente "módulo de interface" é a entidade responsável por notificar as camadas superiores sobre a ocorrência desses eventos.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.30.01: Analisar se a documentação técnica descreve os eventos detectados pela leitora.

EN.II.30.02: Provocar os eventos de inserção e remoção do cartão inteligente, e verificar, por meio de inspeção da leitora e ferramenta específica, as respectivas notificações sobre a ocorrência de cada evento.

REQUISITO II.31: A documentação técnica da leitora deve descrever todos os eventos que podem ser detectados.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.31.01: Verificar se a documentação técnica atende ao **REQUISITO II.31.**

D – Gerenciamento da interface com um cartão inteligente

REQUISITO II.32: O componente "módulo de interface" é responsável por tornar disponível uma interface de tal forma que seja possível requisitar o estado de um cartão inteligente.

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO II.33**.

REQUISITO II.33: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.4, tabela 3-2, as seguintes informações devem estar disponíveis sobre o estado de um dado cartão inteligente:

- Presença de cartão inteligente;
- estado da interface com o cartão inteligente;
- cadeia de caracteres (*string*) ATR;
- tipo de cartão inteligente baseado na seqüência ATR.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.33.01: Analisar a documentação técnica referente a este requisito, verificando as informações retornadas sobre o estado de um cartão inteligente.

EN.II.33.02: Por meio de ferramenta específica via "Módulo de Interface", deve verificar se, no mínimo, as informações descritas no **REQUISITO II.33** estão disponíveis sobre um dado cartão inteligente.

EN.II.33.03: Baseando-se no ensaio **EN.II.33.02**, verificar se as informações retornadas estão em conformidade com o padrão PC/SC versão 1.0, Parte 3, Seção 3.1.4 e Tabela 3-2.

REQUISITO II.34: O SCL, no mínimo, deve ser capaz de distinguir entre dois tipos de erros de comunicação:

- Cartão inteligente inoperante ou sem resposta;
- irrecuperáveis.

Procedimentos de Ensaio para NSH 1:

EN.II.34.01: Verificar se a documentação técnica descreve os erros de comunicação identificados pelo SCL da leitora.

EN.II.34.02: Provocar os erros de comunicação descritos no **REQUISITO II.34**, e depois verificar, por meio de ferramenta específica, se os códigos dos erros provocados são distintos e estão em conformidade com a documentação.

Procedimentos de Ensaio para NSH 2:

EN.II.34.03: Analisar código fonte do driver da leitora, identificando o tratamento dos erros citados no **REQUISITO II.34**.

Procedimentos de Ensaio para NSH 3:

EN.II.34.04: Analisar o código fonte do componente módulo de interface e do firmware da leitora, verificando o tratamento dado aos erros citados no **REQUISITO II.34**.

REQUISITO II.35: Os erros de comunicação devem ser informados ao Provedor de Serviço do cartão inteligente que está logicamente conectado.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.35.01: Verificar se a documentação técnica descreve os erros de comunicação informados ao SP do cartão inteligente que está logicamente conectado.

EN.II.35.02: Provocar possíveis erros de comunicação entre cartão inteligente e PC.

EN.II.35.03: Por meio de uma aplicação específica, tentar realizar operação criptográfica via CSP, verificando o erro de comunicação retornado.

EN.II.35.04: Por meio de uma aplicação específica, tentar realizar operação criptográfica via "Módulo de Interface", verificando se o erro de comunicação retornado pelo SCL é o mesmo daquele retornado no ensaio **EN.II.35.03**.

REQUISITO II.36: A documentação técnica da leitora deve descrever as informações de estado que podem ser obtidas de um cartão inteligente, mostrando de forma clara a estrutura de dados utilizada nas respostas (TLV, por exemplo).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.36.01: Verificar se a documentação técnica atende ao **REQUISITO II.36**.

REQUISITO II.37: A documentação técnica da leitora deve descrever os erros de comunicação que podem ser detectados pelo dispositivo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.37.01: Verificar se a documentação técnica atende ao **REQUISITO II.37**.

E – Suporte a protocolos

A Figura 4 ilustra o fluxo de informações que ocorre entre o SCL e o SP do cartão inteligente. Neste caso, o SCL oculta do nível de aplicação todos os detalhes relacionados aos protocolos.

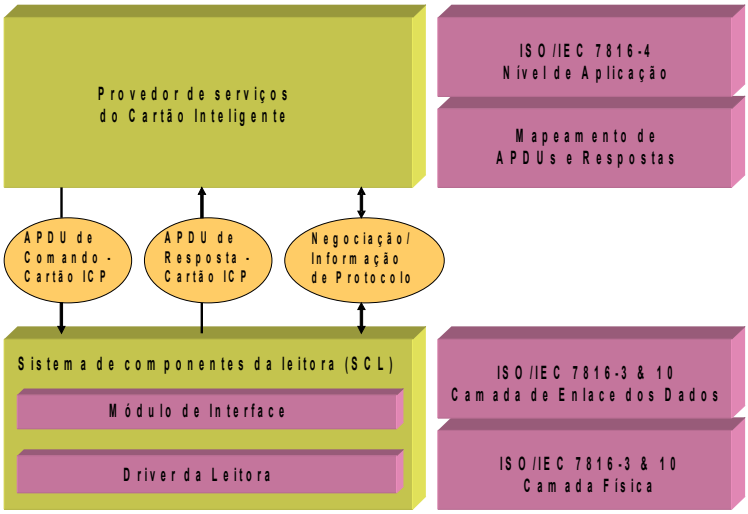

Figura 4. Mapeamento das Camadas ISO/IEC 7816 com o SCL

REQUISITO II.38: Uma leitora deve apresentar as seguintes características:

- Suportar ambos os protocolos, T=0 e T=1;
- suportar uma freqüência CLK normal (*default*) dentro do intervalo 1 a 5 Mhz.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.38.01: Verificar se a documentação técnica descreve o suporte da leitora aos protocolos T=0 e T=1, e a frequência CLK normal.

EN.II.38.02: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com a leitora de cartões inteligentes, e solicitar o envio de instruções PPS pela leitora a um cartão inteligente de teste, por meio de ferramenta específica, para definir os protocolos de transmissão T=0 e T=1 (padrão ISO/IEC 7816-3 – Seções 8 e 9). A seguir, enviar comandos APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

EN.II.38.03: Por meio de ferramenta específica, estabelecer comunicação por meio da interface PC/SC e driver da leitora, e estabelecer conexão lógica com a leitora especificando o protocolo de transmissão T=0 (padrão ISO/IEC 7816-3 - Seção 8). A seguir, enviar comandos

APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

EN.II.38.04: Por meio de ferramenta específica, estabelecer comunicação por meio da interface PC/SC e driver da leitora, e estabelecer conexão lógica com a leitora especificando o protocolo de transmissão T=1 (padrão ISO/IEC 7816-3 - Seção 9). A seguir, enviar comandos APDU ao cartão inteligente observando, por meio de equipamento específico, a estrutura dos dados trocados entre cartão inteligente e leitora.

EN.II.38.05: Inserir um cartão inteligente de teste na leitora observando a frequência CLK aplicada ao cartão. Após a observação, por meio de equipamento específico (por exemplo osciloscópio), da frequência utilizada, verificar a conformidade com o **REQUISITO II.38**.

REQUISITO II.39: Uma leitora deve esperar que uma aplicação primeiro estabeleça uma conexão lógica para depois negociar as configurações necessárias de protocolos.
Requisições de conexão lógica indicam por parte de uma aplicação o protocolo desejado e se os parâmetros de tempo devem ser otimizados ou considerados de acordo com o valor padrão (*default*).

Procedimentos de Ensaio para NSH 1:

EN.II.39.01: Analisar se a documentação técnica descreve os processos de estabelecimento de conexões lógicas e negociações de protocolos entre aplicações e leitoras.
EN.II.39.02: Estabelecer uma conexão lógica com a leitora, por meio de uma aplicação específica, e a seguir verificar as negociações de protocolos de comunicação entre cartão inteligente e leitora por meio de ferramenta específica.

Procedimentos de Ensaio para NSH 2:

EN.II.39.03: Analisar o código fonte do driver da leitora, e verificar como ocorrem os processos de estabelecimento de conexões lógicas e negociações de protocolos entre aplicações e leitoras.

Procedimentos de Ensaio para NSH 3:

EN.II.39.04: Analisar o código fonte do módulo de interface e do firmware da leitora, e verificar como ocorrem os processos de estabelecimento de conexões lógicas e negociações de protocolos entre aplicações e leitoras.

REQUISITO II.40: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.5, tabela 3-4, o componente "módulo de interface" deve tornar disponível uma interface que possibilite ao SP enumerar as configurações de protocolos e os parâmetros disponíveis.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.40.01: Verificar se a documentação técnica descreve as características do componente "Módulo de Interface".

EN.II.40.02: Analisar a interface disponível pelo componente "Módulo de Interface", e depois verificar, por meio de uma ferramenta específica, se é possível enumerar as configurações de protocolos e parâmetros disponíveis em conformidade com a codificação especificada pelo padrão PC/SC versão 1.0, Parte 3, Seção 3.1.5 e Tabela 3-4.

2.3.4.4.2 Funcionalidades opcionais

A – Gerenciamento de energia no cartão inteligente

Uma leitora poderia permitir que um cartão inteligente inserido possa ser ativado e desativado sob o controle do SP.

Tal funcionalidade visa minimizar o consumo de energia, quando o cartão inteligente necessita estar inserido na leitora por um longo período de tempo, embora esteja sendo usado com pouca freqüência.

REQUISITO II.41: A documentação técnica da leitora deve descrever qualquer mecanismo de gerenciamento de energia que esteja implementado no dispositivo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.41.01: Verificar se a documentação técnica atende o **REQUISITO II.41**.

1.1.1.1.1 B – Características específicas do fornecedor

Leitoras podem implementar características que são específicas do fornecedor do dispositivo e cujas funcionalidades não foram definidas nesta especificação.

REQUISITO II.42: Características específicas do fornecedor da leitora devem ser isoladas de tal forma que não causem qualquer impacto nas funcionalidades definidas por este documento (Manual de Condutas Técnicas 2 – Volume I).

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO II.43**.

REQUISITO II.43: Características específicas do fornecedor da leitora devem ser isoladas de tal forma que não permitam que as funcionalidades definidas por este documento (Manual de Condutas Técnicas 2 – Volume I) sejam contornadas ou logradas.

Procedimentos de Ensaio para NSH 1:

EN.II.43.01: Verificar se a documentação técnica descreve detalhadamente as características específicas do fornecedor da leitora, assim como sua estrutura de dados e comandos.

EN.II.43.02: Por meio de aplicação específica, verificar o tráfego de informações entre a leitora e o PC, e verificar se as características específicas do fornecedor da leitora estão presentes.

Procedimentos de Ensaio para NSH 2:

EN.II.43.03: Basear-se nos resultados obtidos no ensaio **EN.II.43.02**, e com a análise do código fonte do driver da leitora, verificar como são tratadas as características específicas do fornecedor da leitora.

Procedimentos de Ensaio para NSH 3:

EN.II.43.04: Basear-se nos resultados obtidos no ensaio **EN.II.43.02**, e com a análise do código fonte do firmware da leitora, verificar o isolamento das características específicas do fornecedor da leitora e se estas oferecem qualquer risco de segurança para as funcionalidades definidas pelo Manual de Condutas Técnicas 2 – Volume I.

REQUISITO II.44: A documentação técnica da leitora deve descrever todas as características que são específicas do fornecedor e estejam implementadas no dispositivo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.44.01: Verificar se a documentação técnica atende ao **REQUISITO II.44**.

2.4 Requisitos de documentação

Os requisitos de documentação dizem respeito aos documentos e suas características que devem acompanhar o objeto de homologação (leitora de cartões inteligentes) na sua forma comercial.

REQUISITO III.1: O responsável deve fornecer, no mínimo, as seguintes informações, em idioma português do Brasil, na documentação que acompanha o objeto de homologação na sua forma comercial:

- Utilização;
- instalação do driver;
- especificações técnicas;
- plataformas de sistemas operacionais compatíveis;
- bibliotecas de softwares disponíveis ou compatíveis.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.III.01.01: Verificar se a documentação que acompanha o produto atende ao **REQUISITO III.1**.

REQUISITO III.2: Toda documentação relacionada a software deve informar as plataformas de sistemas operacionais suportadas e os requisitos de ambiente operacional necessários para sua operação.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.III.02.01: Verificar se a documentação que acompanha o produto atende ao **REQUISITO III.2**.

REQUISITO III.3: Todo software deve:

- Possuir ou possibilitar sua instalação em idioma português do Brasil;
- possuir tópicos de ajuda em idioma português do Brasil;
- permitir a visualização da versão do software e o nome de seu responsável.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.III.03.01: Verificar se os softwares que acompanham o produto atendem ao **REQUISITO III.3**.

REQUISITO III.4: As versões dos componentes de software devem estar descritas à entidade usuária externa na documentação que acompanha o produto.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.III.04.01: Verificar se os softwares que acompanham o produto atendem ao **REQUISITO III.4**.

3 Referências bibliográficas

[ANSI X9.31] AMERICAN NATIONAL STANDARDS INSTITUTE. **Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)**. American Bankers Association. 1998.

[ANSI X9.62] AMERICAN NATIONAL STANDARDS INSTITUTE. **Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA).** American Bankers Association. November 2005.

[CCID 1.1] UNIVERSAL SERIAL BUS. ***Specification for Integrated Circuit(s) Cards Interface Devices.*** *Revision 1.1*. April, 2005.

[FIPS 186-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: *Digital Signature Standard (DSS).*** FIPS PUB 186-2. Washington. US Government Printing Office: Jan. 27, 2000.

[FIPS PUB 140-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules.** FIPS PUB 140-2. Washington. US Government Printing Office: May 25, 2001.

[GLOSSÁRIO ICP-BR] INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS. **Glossário ICP-Brasil.** Versão 1.2. Brasília. ICP – BR: 2007.

[IN 01/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 01/2007: Procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.** DOC-ICP-10.01. Brasília. ICP-Brasil: 2007.

[IN 02/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO.

Instrução normativa 02/2007: Estrutura normativa técnica e níveis de segurança de homologação a serem utilizados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. DOC ICP-10.02. ICP-Brasil: 2007.

[IN 03/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 03/2007: Padrões e procedimentos técnicos a serem observados nos processos de homologação de cartões inteligentes (*smart cards),* leitoras de cartões inteligentes e *tokens* criptográficos no âmbito da ICP-Brasil.** DOC-ICP-10.03. Brasília. ICP-Brasil: 2007.

[ISO/IEC 7816-2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.** Reference Number: 7816-2. Genève, Switzerland: ISO/IEC. 1999(E).

[ISO/IEC 7816-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols.** Reference Number: 7816-3. Genève, Switzerland: ISO/IEC. 1997(E).

[ISO/IEC 7816-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols - AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V.** Reference Number: 7816-3. Genève, Switzerland, ISO/IEC: 1997/Amd. 1:2002(E).

[ISO/IEC 7816-4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange.** Reference Number: 7816-4. Genève, Switzerland, ISO/IEC : 1995(E).

[ISO/IEC 7816-5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers.** Reference Number: 7816-5. Genève, Switzerland, ISO/IEC: 1994(E).

[ISO/IEC 7816-6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements for interchange.** Reference Number: 7816-6. Genève, Switzerland, ISO/IEC: 2004(E).

[ISO/IEC 7816-7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 7: Interindustry commands for Structured Card Query Language (SCQL).** Reference Number: 7816-7. Genève, Switzerland, ISO/IEC: 1999(E).

[ISO/IEC 7816-8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 8: Commands for security operations.** Reference Number: 7816-8. Genève, Switzerland, ISO/IEC: 2004(E).

[ISO/IEC 7816-9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 9: Commands for card management.** Reference Number: 7816-9. Genève, Switzerland, ISO/IEC: 2004(E).

[NIST SP 800-90] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). ***Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised).*** Special Publication 800-90. Washington. US Government Printing Office: March, 2007.

[PC/SC 1.0 Part 2] PC/SC WORKGROUP. **Interoperability Specification for ICCs and Personal Computer Systems – Part 2. Interface Requirements for Compatible IC Cards and Readers.** Version 1.0. PC/SC Specification: Dec, 1997.

[PC/SC 1.0 Part 3] PC/SC WORKGROUP. **Interoperability Specification for ICCs and Personal Computer Systems – Part 3. Requirements for PC-Connected Interface Devices.** Version 1.0. PC/SC Specification: Dec, 1997.

[RSA PKCS#11] RSA LABORATORIES – PKCS#11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD. RSA Security Inc. Version 2.20. June, 2004.

[USB 2.0] UNIVERSAL SERIAL BUS REVISION 2.0 SPECIFICATION – USB-IF.

[RESOLUÇÃO 41 – ICP-BRASIL] COMITÊ GESTOR DA ICP-BRASIL. RESOLUÇÃO N° 41, DE 18 DE ABRIL DE 2006 – REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADOS NA ICP-BRASIL. ICP-BRASIL: Infraestrutura de Chaves Públicas Brasileira. 18 de Abril de 2006.